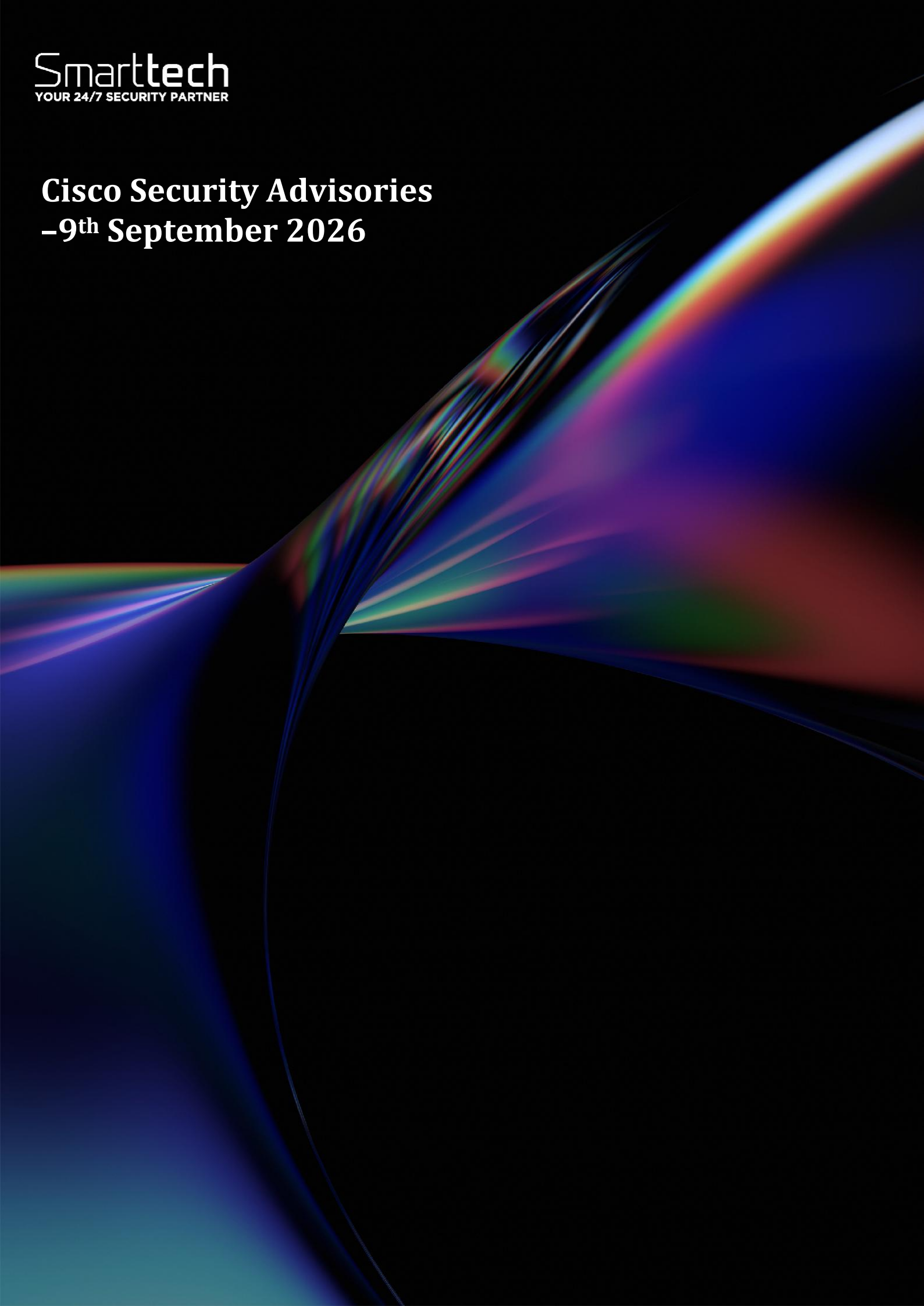
Smarttech
YOUR 24/7 SECURITY PARTNER

Cisco Security Advisories –9th September 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	157
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Catalin Nita < catalin.nita@smarttech247.com >
Last modified	9th September 2026
Issue Date	9th September 2026

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Cisco disclosed a new vulnerability affecting Cisco UCS and UCS-Based Appliances UEFI Shell Secure Boot. This vulnerability could allow attackers to bypass UEFI Secure Boot protections. Successful exploitation could result in the execution of unauthorized software and compromise the integrity of affected systems.

Risk

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Technical summary

CVE-2026-20293
CVSS Score: **7.1**

A vulnerability in the Unified Extensible Firmware Interface (UEFI) Shell implementation of Cisco UCS Servers and UCS-based appliances could allow an authenticated attacker with valid credentials for a user account with the role of user or admin or an unauthenticated attacker with physical access to an affected device to bypass UEFI Secure Boot validation checks and execute unauthorized software.

This vulnerability is due to the availability of memory write commands in the UEFI Shell while UEFI Secure Boot is enabled on a device. An attacker could exploit this vulnerability by selecting the UEFI Shell boot option at boot time and using available shell commands to modify UEFI memory variables. A successful exploit could allow the attacker to manipulate the preboot environment, overwrite UEFI Secure Boot-related memory values, and execute unauthorized software on the affected device.

Affected Products

This vulnerability affects the following Cisco products if they have UEFI Secure Boot enabled and are running a vulnerable BIOS version:

- 5000 Series Enterprise Network Compute Systems (ENCS) (CSCwu42927)
- UCS B-Series Blade Servers (CSCwt77804)
- UCS C-Series Rack Servers (CSCwt77804)
- UCS C845A M8 Rack Server (CSCwt77950)
- UCS C885A M8 Rack Server (CSCwt77952)
- UCS C880A M8 Rack Server (CSCwt78022)
- UCS E-Series M3 Servers (CSCwu42927)
- UCS E-Series M6 Servers (CSCwu42928)
- UCS S-Series Storage Servers (CSCwt77804)
- UCS X-Series Modular System (CSCwt77804)
- Unified Edge (CSCwt77804)

Cisco appliances that are based on a preconfigured version of a Cisco UCS C-Series Server are also affected by this vulnerability if they support UEFI Secure Boot and expose access to the keyboard, video, and mouse (KVM) or virtual KVM console. At the time of publication, this included the following Cisco products:

- Application Policy Infrastructure Controller (APIC) Servers
- Cisco Telemetry Broker Appliances
- HyperFlex Edge Nodes
- HyperFlex Nodes
- IEC6400 Edge Compute Appliances
- IOS XRv 9000 M7 Appliances
- Nexus Dashboard Appliances
- Secure Email Gateways*
- Secure Email and Web Manager*
- Secure Endpoint Private Cloud Appliances
- Secure Firewall Management Center (FMC) Appliances
- Secure Malware Analytics Appliances
- Secure Network Analytics Appliances
- Secure Network Server (ISE SNS) Appliances
- Secure Web Appliances*

**Physical KVM access is required to exploit the vulnerability on these appliances, which significantly reduces the attack vector on these platforms.*

Fixed Releases

5000 Series ENCS

Cisco NFVIS Release	First Fixed Release
4.15 and earlier	4.15.7 (Oct 2026)

Note: *Upgrading Cisco Integrated Management Controller (IMC) and BIOS on Cisco 5000 Series ENCS requires upgrading Cisco Enterprise NFV Infrastructure Software (NFVIS) on the platforms. Cisco IMC and BIOS are upgraded as part of the firmware auto-upgrade process.*

UCS B-Series and X-Series Servers in UCS Manager Mode

Cisco UCS Server Software Release	First Fixed Release
Earlier than 4.3	Migrate to a fixed release.
4.3	4.3(6h)*
6.0	6.0(2d)*

** These releases do not include a fix for Cisco UCS B-Series M5 Servers. A fix for these platforms will be included in upcoming releases (September 2026).*

UCS B-Series Servers in Intersight Managed Mode

Cisco Intersight Server Firmware Release	First Fixed Release
Earlier than 5.4	Migrate to a fixed release.
5.4	5.4(0.260050)*
6.0	6.0(2.260143)

** This release does not include a fix for Cisco UCS B-Series M5 Servers. A fix for these platforms will be included in an upcoming release (September 2026).*

UCS X-Series Servers in Intersight Managed Mode

Cisco Intersight Server Firmware Release	First Fixed Release
Earlier than 5.4	Migrate to a fixed release.
5.4	5.4(0.260042)
6.0	6.0(2.260143)

UCS C845A M8 Rack Server

Cisco UCS Server Software Release	First Fixed Release
2.0	Release no. TBD (Oct 2026)

UCS C880A M8 Rack Server

Cisco UCS Server Software Release	First Fixed Release
4.0	4.0(2.260004)

UCS C885A M8 Rack Server

Cisco UCS Server Software Release	First Fixed Release
1.2 and earlier	Release no. TBD (Sep 2026)

UCS C-Series M5 Rack Servers in Standalone Mode or Intersight Managed Mode

Cisco UCS Server Software Release	First Fixed Release
Earlier than 4.2	Migrate to a fixed release.
4.2	4.2(3r)
4.3	4.3(2.260020)

UCS C-Series M6, M7, M8 Rack Servers in Standalone Mode or Intersight Managed Mode

Cisco UCS Server Software Release	First Fixed Release
Earlier than 4.2	Migrate to a fixed release.
4.2	4.2(3r)
4.3	4.3(6.260054)

6.0	6.0(2.260143)*

**The fixed 6.0(2.260143) Host Upgrade Utility (HUU) ISO release includes the Cisco IMC 6.0(2.260094) packaged release. After upgrading to this fixed release, the Cisco IMC UI Dashboard page will display the Firmware Version as 6.0(2.260094). The Last HSU bundle used field under Administration > Firmware Management will display the fixed 6.0(2.260143) release.*

UCS C-Series Servers in UCS Manager Mode

Cisco UCS Server Software Release	First Fixed Release
Earlier than 4.2	Migrate to a fixed release.
4.2	4.2(3s)
4.3	4.3(6h)*
6.0	6.0(2d)*

** These releases do not include a fix for Cisco UCS C-Series M5 Servers. A fix for these platforms will be included in upcoming releases (September 2026).*

UCS E-Series M3 Servers

Cisco UCSE BIOS Release	First Fixed Release
4.0 and earlier	4.04* (Sep 2026)

** The fixed 4.04 BIOS release can be installed on UCS E-Series M3 Servers that are running any Cisco IMC 3.2 release using the steps in the Managing Firmware section of the Cisco UCS E-Series Integrated Management Controller GUI Configuration Guide.*

UCS E-Series M6 Servers

Cisco UCSE Software Release	First Fixed Release
4.15 and earlier	4.15.4-b* (Sep 2026)

** The fixed 4.15.4-b Host Upgrade Utility (HUU) ISO release includes the fixed 2.06 BIOS release.*

UCS S-Series Storage Server

Cisco UCS Server Software Release	First Fixed Release
Earlier than 4.3	Migrate to a fixed release.
4.3	4.3(6.260054)

Unified Edge

Cisco UCS XE-Series Server Firmware Release	First Fixed Release
6.0	6.0(2.260143)

Note: For Cisco appliances that are based on a preconfigured version of a Cisco UCS C-Series Server, administrators can perform a direct upgrade of the Cisco IMC and BIOS software using one of the fixed releases mentioned in the preceding tables. For instructions, see the Cisco Host Upgrade Utility User Guide. The exceptions are the appliances that are listed in the following table:

Cisco Hardware Platform	First Fixed Firmware Release	Remediation
Cisco Telemetry Broker Appliances	6.0(2.260143)*	Install the firmware update CTB-FIRMWARE-6.0.2.260143-M6.iso.
IEC6400 Edge Compute Appliances	4.3(6.260054)	Apply the HUU upgrade using IEC6400-HUU-4.3.6-260054.img.
IOS XRv 9000 M7 Appliances	6.0(2.260143)*	Upgrade to Cisco IOS XR Software Release 26.3.1, then upgrade the appliance firmware from the Cisco IOS XR CLI.
Secure Email Gateways	4.3(2.260020)	Install the firmware update package (Oct 2026).
Secure Email and Web Manager	4.3(2.260020)	Install the firmware update package (Oct 2026).
Secure Endpoint Private Cloud Appliances	4.3(2.260020) (M5) 4.3(6.260054) (M6)	Follow the steps documented in the TechNote.
Secure Firewall Management Center (FMC) Appliances	4.3(2.260020) (M5) 6.0(2.260143)[1] (M6, M8)	Apply the Hotfix GA.
Secure Malware Analytics Appliances	4.3(2.260020) (M5) 4.3(6.260054) (M6)	Update the firmware using the Out-of-Band Firmware Update ISO procedure.
Secure Network Analytics Appliances	4.3(2.260020) (M5) 6.0(2.260143)[1] (M6)	For M5, install the firmware update patch-common-SNA-FIRMWARE-4.3.2.260020-M5-v2-01.swu. For M6, install the firmware update patch-common-SNA-FIRMWARE-6.0.2260143-M6-v2-01.swu.
Secure Network Server (ISE SNS) Appliances	4.3(2.260020) (M5) 6.0(2.260143)[1] (M6, M8)	Apply the BIOS and HUU upgrade, as documented in Firmware Upgrade Guide for Cisco Secure Network Server 3600 Series, Cisco Secure Network Server 3700 Series, or Cisco Secure Network Server 3800 Series.
Secure Web Appliances	4.2(3r) (M5) 4.3(6.260054) (M6)	Install the firmware update package (Oct 2026).

** The fixed 6.0(2.260143) firmware release includes the Cisco IMC 6.0(2.260094) packaged release. After upgrading to this fixed release, the Cisco IMC UI Dashboard page will display the Firmware Version as 6.0(2.260094). The Last HSU bundle used field under Administration > Firmware Management may display the fixed 6.0(2.260143) release or N/A, depending on the specific appliance and remediation used.*

Recommendations

The **Smarttech247** team recommends the following actions**:**

- Apply the security updates provided by Cisco and upgrade all affected Cisco instances to a fixed software release as soon as operationally feasible. Cisco has indicated that no workarounds are available for these vulnerabilities.
- Implement the Principle of Least Privilege by limiting administrative access and regularly reviewing user accounts, roles, and permissions assigned within the SD-WAN environment.
- Monitor system and authentication logs for signs of unauthorized privilege escalation

attempts, suspicious administrative activity, or unexpected configuration changes, and forward logs to a centralized logging platform for analysis.
- Use vulnerability management and security monitoring solutions to identify affected systems, verify remediation status, and detect potential exploitation attempts.
- Ensure endpoint, network, and security monitoring solutions are up to date to provide visibility into malicious activity targeting SD-WAN infrastructure and management components.

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-uefi-sb-bypass-eb6xC5GW

CVE

CVE-2026-20293

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com